NANOSYSTEMS:
PHYSICS, CHEMISTRY, MATHEMATICS

Original article

Deepika Aggarwal, et al. *Nanosystems: Phys. Chem. Math.*, 2025, **16** (5), 597–605.
http://nanojournal.ifmo.ru
DOI 10.17586/2220-8054-2025-16-5-597-605

Unpredictable and uniform random number generation based on time of arrival using InGaAs detectors

Deepika Aggarwal[1,a], Anindita Banerjee[1,b], Ankush Sharma[1,c], Ganesh Yadav[1,d]

[1]QuNu Labs Pvt. Ltd., M.G. Road, Bangalore, Karnataka, India

[a]deepika@qnulabs.com, [b]anindita@qnulabs.com, [c]ankush@qnulabs.com, [d]ganesh@qnulabs.com

Corresponding author: Deepika Aggarwal, deepika@qnulabs.com

ABSTRACT Quantum random number generators are becoming mandatory in a demanding technological world of high-performing learning algorithms and security guidelines. Our implementation, based on the principles of quantum mechanics, enables us to achieve the required randomness. We have generated high-quality quantum random numbers from a weak coherent source at the telecommunication wavelength. The entropy is based on the time of arrival of quantum states within a predefined time interval. The detection of photons by the InGaAs single-photon detectors and high-precision time measurement of 5 ps enables us to generate 16 random bits per arrival time, which is the highest reported to date. We have presented the theoretical analysis and experimental verification of the random number generation methodology. The method eliminates the requirement of any randomness extractor, thereby leveraging the principles of quantum physics to generate random numbers. The output data rate averages 2.4 Mbps. The generated raw quantum random numbers are compared with the NIST-prescribed Blum-Blum-Shub pseudo-random number generator and an in-house-built hardware random number generator from FPGA, on the ENT and NIST platform.

KEYWORDS random number generation, InGaAs detector.

FOR CITATION Deepika Aggarwal, Anindita Banerjee, Ankush Sharma, Ganesh Yadav Unpredictable and uniform random number generation based on time of arrival using InGaAs detectors. *Nanosystems: Phys. Chem. Math.*, 2025, **16** (5), 597–605.

1. Introduction

In the present era, random numbers play a significant role in statistical analysis, stochastic simulations, cyber security applications, gaming, cryptography and many others. Random numbers can be generated via two approaches: pseudo-random number generators (PRNGs) [1], which rely on deterministic algorithms, and true random number generators (TRNGs), which derive randomness from physical processes. While PRNGs risk predictability due to seed reuse or algorithmic backdoors, TRNGs leverage physical entropy sources. Quantum random number generators (QRNGs), a subset of TRNGs, exploit the inherent unpredictability of quantum mechanics to produce unbiased and irreproducible outputs.

A random bit sequence is characterized by two fundamental properties, i.e., uniformity and unpredictability, of which the latter is the most important. Uniformity is achievable by mathematical algorithms, however, for unpredictability, none other than the inherent randomness of quantum mechanics can be trusted. Quantum random numbers can be generated from several sources, for example, radioactive decay [2, 3], branching path [4], photon arrival times [5–9], quantum vacuum fluctuations [10–14], laser phase fluctuations [15, 16], optical parametric oscillators [17], amplified spontaneous emission [18] etc. Several optical QRNG schemes [19] have been proposed on the principle of time of arrival (ToA) of photon. The arrival time of photon is considered as a quantum random variable and it can generate n random bits, where, n depends on the precision of time measurement. Software [6, 7, 20] and hardware [21] approaches were investigated to eliminate the bias and improve the quality of throughput from the time of arrival entropy. The authors in [8] showed that when an external time reference is used, the raw random numbers are generated from the photon arrival in time bins within the external time reference and are uniformly distributed in time. Hence, we can consider this quantum entropy source to be one of the ideal candidates for TRNG.

In this paper, we have reported our work on QRNG based on ToA principle using an external time reference. We have implemented the scheme using InGaAs detectors. We have used a different method for generating random numbers and could extract 16 random bits per detection event. This is the highest reported entropy per detection event among time-of-arrival based QRNGs. In our work, we have adhered to the quantum noise random number generator architecture recommended by ITU-T X.1702 [22] and this is presented in Fig. 1. The raw data is extracted by performing a measurement on a quantum state and we are deriving the random numbers from the data acquisition process. Minimum entropy is accessed by estimating the implementation imperfections. The quantum state is prepared using an optical process and the quantum measurement is based on the Poisson nature of photon detection by single-photon detector (SPD). Raw data

is generated by digitizing the output from the SPD. Continuous monitoring of laser parameters, detector parameters and amplitude of the quantum signal at the detector enables assessment of entropy for evaluation of quantum randomness in the random number sequence. The implementation imperfections lead to an increase in the classical noise, therefore, these are identified, continuously monitored and eliminated.

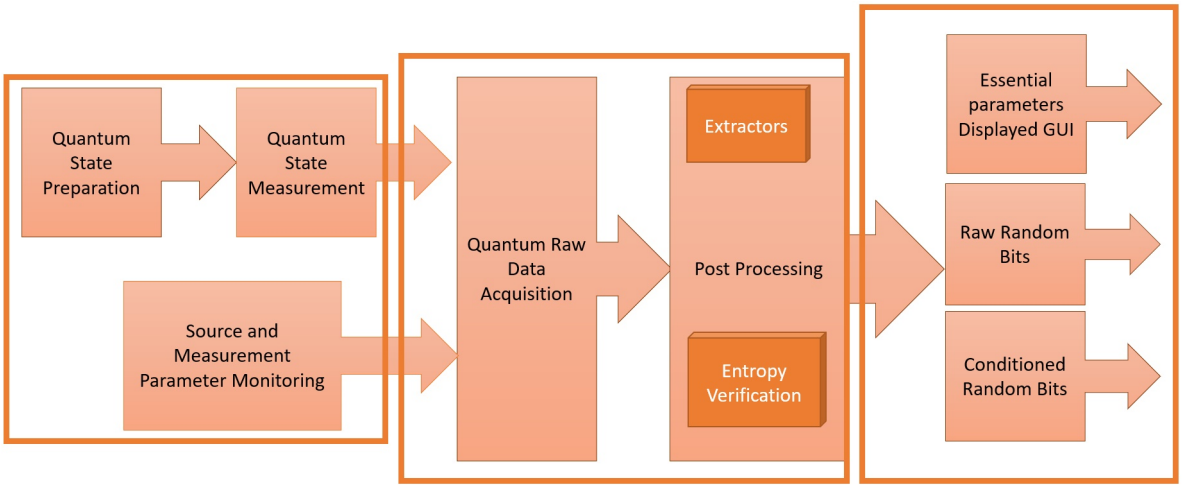

FIG. 1. Schematic of the quantum random number generator architecture. The process involves quantum state preparation using a coherent source, photon detection via InGaAs single-photon detectors, and continuous parameter monitoring to ensure entropy quality. Time-of-arrival measurements generate raw data, which undergoes direct processing and entropy verification to guarantee uniformity and unpredictability. Post-processed bitstreams and essential parameters are displayed through a graphical user interface (GUI) [22]

Section 2 of this paper explains the source of quantum randomness. In section 3, we have discussed the principle of time of arrival along with its theoretical analysis and sources of bias in the implementation. Section 4 presents the experimental setup and section 5 discusses the entropy estimation. Finally, we have concluded the work in section 6.

2. Source of randomness

The quantum randomness in the presented QRNG arises from the collapse of the coherent state during photon detection. Since our QRNG method is based on the ToA principle, it is important to briefly discuss the coherent state and present a mathematical description of the photon. The coherent state α is the quantum mechanical counterpart of monochromatic light. It can be represented by amplitude and phase, $\alpha = |\alpha| e^{i\theta}$, where the complex number specifies the amplitude in photon number units. The coherent state can be represented in Dirac notation as $|\alpha\rangle$. The wave function of a highly attenuated laser state (coherent state) can be represented as a product of all the coherent states within the coherence time,

$$|\phi\rangle = \bigotimes_{t=1}^{n_c} |\alpha_t\rangle \tag{1}$$

where, n_c is the number of time bins within the coherence time of the laser. The Fock-state representation of a coherent state distributed over n_c time bins can be written as

$$|\phi\rangle = \sum_{k=0}^{\infty} \sqrt{P_k} \left(\frac{1}{\sqrt{n_c}} \sum_{t=1}^{n_c} a_t^\dagger \right)^k |0\rangle, \tag{2}$$

where $P_k = e^{-n_c\mu}(n_c\mu)^k/k!$ is the Poisson probability of having k photons with mean photon number $n_c\mu$, and $a_t^\dagger$ is the photon creation operator in the t-th time bin. This equation shows that each photon is in a superposition of all time bins, and the collapse of the wavefunction upon detection gives rise to intrinsic quantum randomness.

2.1. Photon statistics within a time segment

It is known that the photon number distribution of perfectly coherent light within a fixed time segment follows a Poisson distribution [23]. Consider a beam segment corresponding to a predefined time segment with an average photon count represented by $\mu = \phi T$, where ϕ is the average optical flux. We divide the time segment into small time bins. It is then demonstrated that the probability of finding n photons within a time segment (T) containing N time bins follows a Poisson distribution. Let the probability of detecting n photons within the time segment T be represented by $P(n)$. Consider the probability of finding n time bins containing 1 photon and $N-n$ time bins containing no photons, which is denoted as p_1 and calculated as $p_1 = \mu/N$. This probability is given by a binomial distribution,

$$\begin{aligned} P(n) &= \frac{N!}{n!(N-n)!} p_1^n (1-p_1)^{N-n} \\ &= \frac{N!}{n!(N-n)!N^n} \mu^n \left(1-\frac{\mu}{N}\right)^{N-n}. \end{aligned} \tag{3}$$

In the limit $N \to \infty$, the probability is $\lim_{N\to\infty}[P(n)] = \frac{1}{n!}\mu^n e^{-\mu}$. Thus, the probability of finding n photons in the time segment T follows a Poisson distribution, denoted as $P(n)$. It is important to mention that we have considered ideal detectors with $100\,\%$ efficiency.

2.2. Quantum theory of photon detection

When conducting an experiment to leverage the Poisson nature of photon statistics of coherent light, we have to consider the optical losses and imperfections in the devices. These are inefficient optics, absorption and imperfect detectors. These lead to a random sampling of photons, which degrades the photon statistics. The quantum theory of photon detection [23] establishes a connection between the photon count statistics recorded by the detector within a time segment T and the photon statistics incident upon the detector. The variance in the photo count number is denoted by $(\triangle C)^2$ and the variance in the photon number is denoted by $(\triangle n)^2$. The relationship between these two parameters is established by

$$(\triangle C)^2 = \eta^2 (\triangle n)^2 + \eta(1-\eta)\mu. \tag{4}$$

If the detector was perfect (i.e. $\eta = 1$), then the photon count statistics would have been equal to the photon statistics. Consider a coherent source with $(\triangle n)^2 = \mu$ and an imperfect detector, such as a PMT or SPAD. In this case, equation 4 becomes $(\triangle C)^2 = \mu\eta = C$. Thus, the photo count statistics (C) and the photon statistics (μ) both follow the Poisson distribution for all values of detection efficiencies.

3. Time of arrival generators

ToA-based QRNG systems encode the arrival time of photons. During the short time periods, the arrival of a photon at the detector follows an exponentially distributed time, $\lambda e^{-\mu T}$. The time between the two arrivals is the difference between two exponential random variables, which is also exponential. The randomness in the exponential distribution can be converted to a uniform bit sequence using post-processing algorithms. Another approach to flatten the exponential distribution is by taking short time bins from an external reference and considering the time of arrivals within those bins. Nie *et al.* [8] have explained that when randomness is extracted from the arrival time, the generated random numbers are biased. They have proposed a new method to generate uniform random numbers from photon clicks within a fixed time duration $(t, t+T)$. The fixed time period is divided into small time bins with precision t_{min}. The time period is always less than the dead time of the detector, allowing single detection. This method offers advantages of low bias and high throughput compared to other methods of quantum random number generation.

3.1. Theoretical analysis

The photon flux, which is an average number of photons passing through a cross-section of a coherent beam, follows a Poisson process. Precisely, a coherent beam with well-defined average photon number will exhibit photon number fluctuation in a short time interval. This fluctuation occurs because we cannot predict the positions of these photons. Consider a 1550 nm laser emitting 0 dBm of power, this will have an average flux of 7.78×10^{15} photons s^{-1}. If we apply 60 dB attenuation to this, the average flux will then be 7.7×10^9 photons s^{-1}. We can interpret this as an average of 7.7 photons in the 1 ns time segment. Also, consider a time segment of 100 ps, corresponding to an average flux of 0.77. To summarize, if the coherent beam is attenuated to an extent that the beam segment contains few photons, say, on an average of 0.77 photons and we make measurements of some n samples, then, one can observe the random fluctuations in the photon number. This comes from the fact that the stimulated emission in the semiconductor laser is inherently random. Considering a time segment T, with mean photon number of μT, then the probability distribution of k photons arriving in time interval T is given by $P(k) = \frac{e^{-\lambda \mathrm{T}}(\mu T)^k}{k!}$. The photon number follows a Poisson distribution. Hence, the time interval between the arrival of consecutive photons also follows the Poisson process [6]. For $\lambda T = 0.1$, there is 90.5%

probability of detecting no photons, 9% of detecting single photons and finite probability of 0.5% of detecting multi-photons in time segment T. The time period is divided into N_b time bins and each time bin is $\tau_i = \left(\frac{i-1}{N_b}T, \frac{i}{N_b}T\right)$. In the case of an ideal detector ($\eta = 1$), there would have been multiple clicks in T, and the first detection would be the minimum value of the random variable representing photon arrival times. However, since the dead time of the detector is more than T, there is a single detection in T. For a detection event, the conditional probability of getting a detection at i^{th} position, given k photons appear in period T, is given by $P(i\,|k)$. It represents the probability of a detection occurring at τ_i when k photons are present in a period,

$$\begin{aligned} P(i \mid k) &= \frac{P(i,k)\cdot P(T-\tau_i, k=0)}{P(k)} \\ &= \frac{\frac{e^{-\lambda\tau_i}\left(\lambda\left(\frac{T-(i-1)T}{N_b}-\frac{T-iT}{N_b}\right)\right)^k}{k!}\cdot e^{-\lambda(T-\tau_i)}}{\frac{e^{-\lambda T}(\lambda T)^k}{k!}} \\ &= \left(\frac{1-(i-1)}{N_b}-\frac{1-i}{N_b}\right)^k \\ &= \left(\frac{1-(i-1)}{N_b}\right)^k - \left(\frac{1-i}{N_b}\right)^k. \end{aligned} \tag{5}$$

The probability distribution function of the arrival of a photon conditioned on the fact that only 1 photon is available in the time period T is (substituting k=1 in equation 5)

$$P(i|k=1) = \frac{1}{N_b} = \frac{1}{T/\tau} = \frac{\tau}{T}, \tag{6}$$

which clearly shows that the photon arrival time is uniformly distributed across all N_b bins of the interval T and the probability of a photon arriving at each time bin is $\frac{1}{N_b}$ [8, 9]. In this expression, τ is the independent variable of the probability distribution function. The probability density is given by $\frac{1}{T}$. Thus, the arrival time is uniformly distributed in $[0, T]$.

We have used binary code to encode the time bins. In Fig. 2, we have presented different methods for implementing time of arrival based QRNG. Wayne *et al.* [6] extracted random numbers by translating the time interval between detections into time bins. Nie *et al.* [8] generated raw quantum random numbers by considering time difference between the photon click and an external time reference. The distribution of time difference between the photon click and the external reference clock is approximately uniform. Yan *et al.* [9] have generated the highest-reported raw data bits of 128 Mbps by measuring the time of arrival from a common starting point. They have converted each arrival time into sum of fixed period and phase time. Thereafter, they have generated random numbers from the phase time. In this work, we address the arrival time of photon differently; we have considered an external time reference for the generation of raw bits. We have divided the external time reference T into N_T divisions. The arrival time is given by

$$A_n = \text{mod}[N_b, N_{T_i}], \tag{7}$$

where N_b is the total number of random digits that we want to generate. We do not restrict ourselves to modular arithmetic; rather, the purpose is to divide the time segment T into N_T fragments, with each fragment equal to the precision of the measurement device. These fragments are divided into N_b divisions to generate N_b random digits. The arrival of a photon will randomly fall within the range $1 \leq N_{T_i} \leq N_T$. Thus, applying equation 7, we can prove that N_{T_i} is uniformly distributed in $[0, T)$ [6, 8]. Table 1 compares the proposed work with existing works.

TABLE 1. Comparison of the proposed QRNG with existing works on the basis of the nature of source, detector, external reference clock, entropy per detection, precision of time measurement and throughput. CS stands for coherent source

Reference	Source	Detector	External reference clock	Entropy	Resolution	Rate (Mbps)
[6]	LED	SiAPD	—	5.5	5 ns	40
[8]	CS	SiAPD	40.96 ns	8	0.160 ns	109
[9]	CS	SiAPD	20 ns	8	20 ns	128
This work	CS	InGaAs	500 ns	16	0.005 ns	2.4

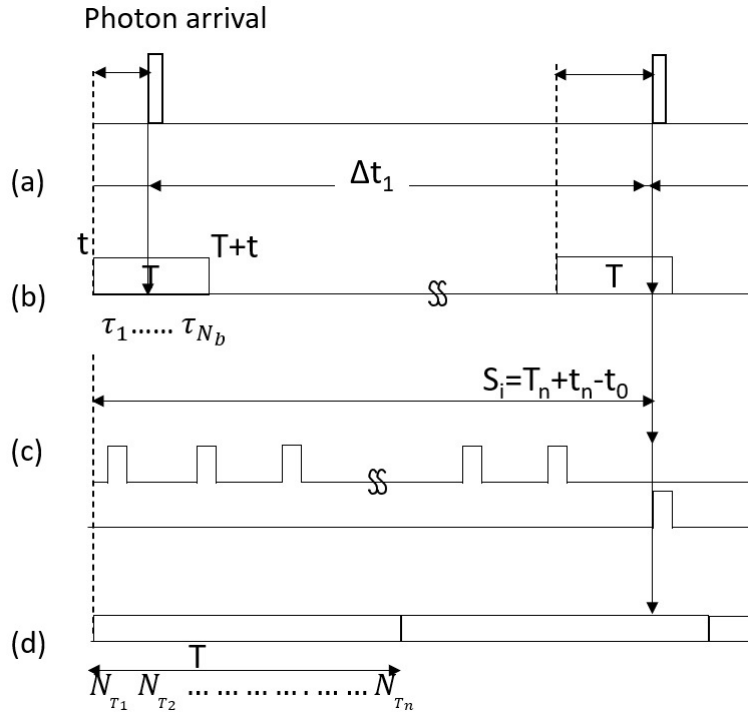

FIG. 2. Timing diagrams for photon arrival time methods: (a) Wayne *et al.* [6] uses intervals Δt_1 between detections; (b) Nie *et al.* [8] employs an external reference clock (SS: start signal); (c) Yan *et al.* [9] measures phase time relative to a fixed period; (d) Proposed method divides external reference T into N_T bins. Gray rectangles represent detection events, and dashed lines mark time bins

3.2. Source of bias

To quantitatively evaluate the randomness of the raw data, we need to model the system carefully and figure out the facts that would introduce bias. There are a few major device imperfections to be examined.

(1) The laser intensity must remain constant. We have analyzed the number of detections per $101\,\mu s$ to validate that the average photon count statistics is uniform. For an average photon number of 0.1 for 100 ns duration and a $10\,\mu s$ detector dead time, there should be one detection every 10100 ns or 10 detections every $101\,\mu s$. We take 100 samples of $1010\,\mu s$ interval to validate the mean photon number (this sample size is enough to ensure statistical confidence of photon statistics).

(2) Detector dark counts are random clicks in the absence of photons. Analyzing the effect of random noise from dark counts mixed with random numbers generated from photon arrival times would be insightful. The dark count rate (350–400 cps) is much less than the detection rate. Such negligible dark counts do not measurably affect uniformity or bias in raw data.

(3) In one of our implementations, we have considered a dead time of $5\,\mu s$, far greater than the duration of external reference, which is 100 ns. The dead time can be considered as a drift [8] and it does not affect the quality of random numbers.

(4) The probability for multi-photon emission from an attenuated continuous-wave (CW) laser is non-zero. If we use detectors capable of distinguishing between multi-photon and single-photon events, we can discard the multi-photon cases. This would reduce bias in the output. However, considering the mean photon number much less than 1 significantly reduces the chances of multi-photon events.

4. Experimental analysis

The experimental setup is presented in Fig. 3. It comprises a distributed feedback laser (DFB) operated in continuous mode with a wavelength of 1550 nm and an output power of 0.1 mW. We have two variable optical attenuators (VOAs) to adjust the amplitude of the weak coherent source to the desired value. One of them is kept fixed and the other is altered to achieve granularity. We have implemented SPD from CHAMPION Aurea in free-running mode. It has the flexibility of adjusting at variable efficiencies, for example, 10%, 20% and 30%. The dead time can be configured to achieve the required count rate for a specific efficiency. We have considered different values of N_b as 8, 100, 200, 256, 500 and 512 for an external clock of 100 ns. When we implemented the scheme with 500 ns clock reference, we have considered 65536 divisions and generated 16 bits per detection. This implies that each division is 7.6 ps. The jitter in the SPD is 180 ps, which ideally suggests that a division size greater than this period should be considered to mitigate timing uncertainty.

In our current experiments, we did not implement larger division sizes, but we fully recognize this approach's importance and will incorporate it into future experiments to improve randomness quality. At 10% efficiency and 10 μs dead time, the SPD recorded a dark count rate of 350-400 cps and a photon count rate of 90 Kcps, corresponding to a photon flux at the input of approximately 9×10^6 cps (equivalent to -89 dBm optical power) with a mean photon count of 0.09. In a separate experimental run with increased photon flux (achieved by adjusting the variable optical attenuator), the SPD count rate reached 96 Kcps, corresponding to 2.4×10^7 cps at the input and a mean photon count of 0.24 (-85 dBm). The adjustments in the optical attenuation settings between these runs were manual and static, not dynamically dependent on input optical power. In continuous operation, we have considered the SPD count rate as 9×10^4 cps. Fig. 4 presents the probability distribution of the generated random digits 1 to 256. We find that the throughput is almost uniform. We converted this data to binary and then tested it on the NIST and ENT test platforms [24, 25]. The dataset used for these tests comprised approximately 1 gigabit of raw quantum random data. At 5 μs dead time, we have considered a counting rate of 150 Kcps. A field-programmable gate array (FPGA) (Zynq UltraScale+ MPSoC) does the post-processing of the data. It also incorporates a time-to-digital converter (TDC) (TDC_AS6501), which can respond to an external clock reference from 2 MHz to 12.5 MHz. The TDC has an internal clock of 5 ps and can count till 500 ns. An external clock reference with frequency 10 MHz in one implementation and 2 MHz in other implementation, with a jitter of 3 ps is used as a reference clock and is edge synchronized with the TDC counter. The throughput at 150 Kcps count rate is 2.4 Mbps (raw QRNG data) with $5\mu s$ dead time.

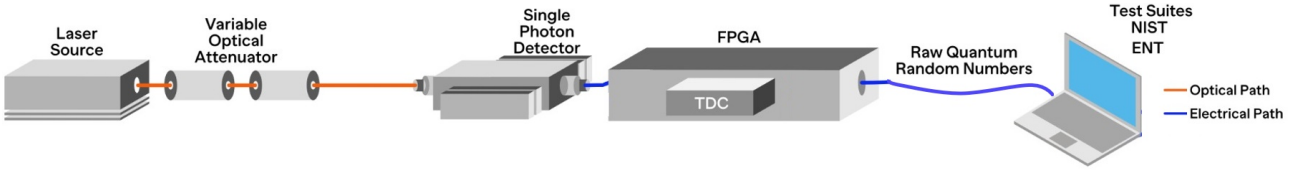

FIG. 3. Experimental setup

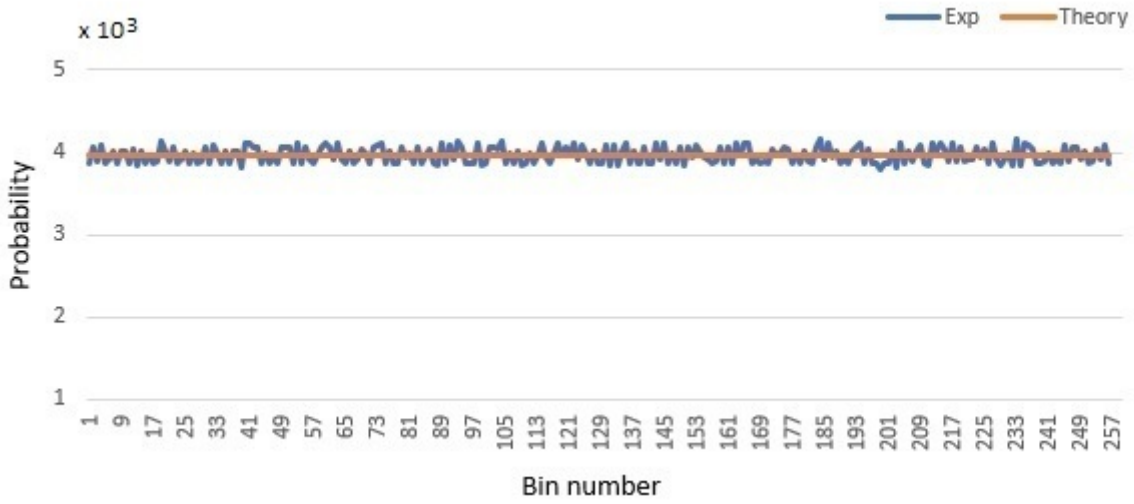

FIG. 4. Probability distribution for theoretical versus experimental values for 256 time bins with 90 Kb of raw data

5. Entropy estimation

Entropy in the information-theoretic sense is a measure of the randomness or unpredictability of the outputs of an entropy source. The larger the entropy, the greater the uncertainty in predicting the outcomes [26]. Estimating the amount of entropy available from a source is necessary to determine how many bits of randomness are available. If a discrete random variable X has n possible values, where the i^{th} outcome has probability p_i, then the Rényi entropy of order α is defined as [27]

TABLE 2. Results of ENT tests

ENT test item	QRNG	TRNG	Ideal value
Entropy (bits per bit)	1.000000	1.000000	1.000000
Chi-square distribution	45 %	15.11 %	10 % $\sim$ 90 %
Arithmetic mean value	0.4997	0.5001	0.5000
Monte Carlo value for Pi	3.1515369080	3.142180307	3.1415926536
Serial correlation coefficient	0.000590	0.000088	0.000000

TABLE 3. Results of NIST tests

NIST test item	BBS	QRNG	TRNG
	p-value	p-value	p-value
Frequency	0.816537	0.534146	0.213309
Block frequency	0.366918	0.122325	0.015598
Cumulative sums	0.955835	0.634146	0.851383
Runs	0.090936	0.739918	0.137282
Longest run	0.202268	0.534146	0.494392
Rank	0.202268	0.534146	0.383827
FFT	0.275709	0.350485	0.494392
Non overlapping template	0.764295	0.991468	0.883171
Overlapping template	0.455937	0.350485	0.779188
Universal	0.060806	0.213309	0.699313
Approximate entropy	0.971699	0.839918	0.739918
Random Excursions	0.534146	0.739918	0.186566
Random Excursions Variant	0.911413	0.457799	0.311542
Serial	0.739918	0.911413	0.779188
Linear complexity	0.145326	0.739918	0.289667

$$H_\alpha(X) = \frac{1}{1-\alpha}\log_2\left(\sum_{i=1}^{n} p_i^\alpha\right), \tag{8}$$

for $0 \leq \alpha \leq \infty$. As $\alpha \to \infty$, the Rényi entropy of X converges to the negative logarithm of the probability of the most likely outcome, called the min-entropy,

$$H_\infty(X) = \lim_{\alpha\to\infty} H_\alpha(X) = -\log_2 \max p_i. \tag{9}$$

The name min-entropy (H_∞) stems from the fact that it is the smallest in the family of Rényi entropies. In this sense, it is the most conservative approach to measuring the unpredictability of a set of outcomes or the randomness content of a distribution. The standard Shannon entropy, which measures the average unpredictability of the outcomes, offers only a rough estimation of randomness. On the other hand, H_∞ is used as a worst-case measure of the uncertainty associated with observations of X. It represents the best-case scenario for an adversary trying to guess an output from the noise source. For H_∞, p_i represents the detection probability at the i^{th} time bin and

$$H_\infty = -\frac{\log_2 P_{\max}}{\log_2 N_b} = 0.9971 \tag{10}$$

from the maximum frequency of 0.00397, which is higher than [8]. The maximum probability $P_{\max}$ was computed as the normalized frequency of the most populated time bin in the photon arrival histogram. As depicted by Fig. 4, the frequency distribution is almost uniform and the experimental values are close to the theoretical values.

We tested the QRNG output using ENT program and NIST test suite. ENT program computes some important statistical properties of the generated random bit-streams. It is a series of basic statistical tests that evaluate the random sequence by some elementary features such as the equal probabilities of ones and zeros, the serial correlation, etc. Testing results with ENT performed on a 1 GB dataset are presented in Table 2. The ENT test results indicate high-quality randomness, with only slight variations in arithmetic mean and serial correlation. These small deviations are attributed to residual classical noise sources. Each test in the NIST suite evaluates a p-value which should be larger than the significance level. The significance level in the tests is $\alpha = 0.01$. The test is considered successful if all the p-values satisfy $0.01 \leq$ p-value ≤ 0.99. In the tests producing multiple outcomes of p-values, the worst outcomes are selected. Testing results with NIST conducted on a 1 GB dataset are presented in Table 3. All the output p-values are larger than 0.01 and smaller than 0.99, which indicates that the generated random bits well pass the NIST tests. ENT and NIST were selected for initial validation due to their broad acceptance and comprehensive coverage of randomness properties. However, future work will expand the analysis to include other test suites as well to further ensure the robustness of the QRNG output. We have also compared raw quantum random numbers with the random numbers generated from NIST's Blum-Blum-Shub (BBS) algorithm and an in-house TRNG built from FPGA based on the asynchronous sampling of a ring oscillator.

6. Conclusion

We have designed and tested a practical high-speed QRNG based on the time-of-arrival quantum entropy from a CW laser at telecommunication wavelength. This study is the first to explore time-of-arrival QRNG using InGaAs detectors. These detectors have a greater dead time than silicon detectors, enabling us to increase the external reference time to 500 ns compared to previous values of 40.6 ns [8] and 20 ns [9]. We have implemented precision time measurement of 5 ps, which is reported here for the first time. Hence, we could extract 16 bits of entropy from one photon arrival time. The photon arrival time follows a Poisson distribution; an exponential waiting time introduces bias, which is overcome using an external reference clock. We successfully generated uniform random numbers with high entropy, particularly min-entropy always greater than 0.99 value. The method of time measurement of photons is simpler in implementation and higher in precision time measurement than earlier works [6,8,9]. We propose that implementing the time-of-arrival QRNG with InGaAs detectors and high precision time measurement will enable generating maximum entropy per detection event. The proposed work can be used to generate higher throughput by increasing the duration of the external reference clock; however, the increase in throughput will be linear. The proposed work also eliminates the need for any mathematical algorithm to generate uniform output; thus, the random numbers produced are derived from the quantum behavior of photons and are truly random.

References

[1] Knuth D.E. *Art of Computer Programming*, Volume 2: Seminumerical Algorithms, Addison-Wesley Professional (2014).

[2] chmidt H. Quantum-mechanical random-number generator, *J. Appl. Phys.*, 1970, **41**, P. 462–468.

[3] Aggarwal D., Ghatikar R., Chennuri S. and Banerjee A. Generation of 1 GB full entropy random numbers with the enhanced-NRBG method. *Physica Scripta*, 2023, **98**(12), P. 125112.

[4] Jennewein T., Achleitner U., Weihs G., Weinfurter H. and Zeilinger A. A fast and compact quantum random number generator. *Rev. Sci. Instruments*, 2000, **71**(4), P. 1675–1680.

[5] Stipcevic M. and Rogina B.M. Quantum random number generator based on photonic emission in semiconductors. *Rev. Sci. Instrum*, 2007, **78**, P. 045104.

[6] Wayne M.A., Jeffrey E.R., Akselrod G.M. and Kwiat P.G. Photon arrival time quantum random number generation. *J. Mod. Opt.*, 2009, **56**(4), P. 516–522.

[7] Wahl M., Leifgen M., Berlin M., Röhlicke T., Rahn H.-J. and Benson O. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Appl. Phys. Lett.*, 2011, **98**, P. 171105.

[8] Nie Y., Zhang H., Zhang Z., Wang J., Ma X., Zhang J. and Pan J. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Appl. Phys. Lett.*, 2014, **104**, P. 051110.

[9] Yan Q., Zhao B., Hua Z., Liao Q. and Yang H. High-speed quantum-random number generation by continuous measurement of arrival time of photons. *Rev. Sci. Instrum.*, 2015, **86**, P. 073113.

[10] Gabriel C., Wittmann C., Sych D., Dong R., Mauerer W., Andersen U.L., Marquardt C. and Leuchs G. A generator for unique quantum random numbers based on vacuum states. *Nat. Photonics*, 2010, **4**, P. 711–715.

[11] Shen Y., Tian L. and Zou H. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A*, 2010, **81**, P. 063814.

[12] Symul T., Assad S.M. and Lam P.K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.*, 2011, **98**(23), P. 145.

[13] Bruynsteen C., Gehring T., Lupo C., Bauwelinck J. and Yin X. 100-Gbit/s integrated quantum random number generator based on vacuum fluctuations. *PRX Quantum*, 2023, **4**, P. 010330.

[14] Raffaelli F., Ferranti G., Mahler D.H., Sibson P., Kennard J.E., Santamato A., Sinclair G., Bonneau D., Thompson M.G. and Matthews J.C.F. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. *Quantum Sci. Technol.*, 2018, **3**, P. 025003.

[15] Guo H., Tang W., Liu Y. and Wei W. Truly random number generation based on measurement of phase noise of a laser. *Phys. Rev. E*, 2010, **81**, P. 051137.
[16] Qi B., Chi Y.-M., Lo H.-K. and Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt. letters*, 2010, **35**(3), P. 312–314.
[17] Marandi A., Leindecker N.C., Vodopyanov K.L. and Byer R.L. All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators. *Opt. Express*, 2012, **20**, P. 19322–19330.
[18] Williams C.R.S., Salevan J.C., Li X., Roy R. and Murphy T.E. Fast physical random number generator using amplified spontaneous emission. *Opt. Express*, 2010, **18**, P. 23584–23597.
[19] Herrero-Collantes M. and Garcia-Escartin J.C. Quantum random number generators. *Rev. Mod. Phys.*, 2017, **89**, P. 015004.
[20] Li S., Wang L., Wu L.-An, Ma H.-Q. and Zhai G.-J.True random number generator based on discretized encoding of the time interval between photons. *J. Opt. Soc. Am. A*, 2013, **30**, P. 124.
[21] Wayne M.A. and Kwait P.G. Low-bias high-speed quantum random number generator via shaped optical pulses. *Opt. Express*, 2010, **18**, P. 9351.
[22] Series X: Data Networks Open System Communications and security, Quantum communication Quantum noise random number generator architecture, Recommendation X.1702 (11/19).
[23] Fox M. *Quantum optics: an introduction*. Oxford Univ. Press, Oxford, Oxford master series in atomic, optical, and laser physics, 2006.
[24] Bassham III L.E., et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-22 Rev. 1a, 2010.
[25] Walker J. ENT: A pseudo-random number sequence test program. http://www.fourmilab.ch/random/ (2008).
[26] Yuan X., Zhao Q., Girolami D. and Ma X. Quantum coherence and intrinsic randomness. *Advanced Quantum Technologies*, 2019, **2**(11), P. 1900053.
[27] A. Rényi. On Measures of Entropy and Information. Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics, P. 547–561, University of California Press, Berkeley, Calif., 1961.

Submitted 1 August 2025; revised 24 August 2025; accepted 25 August 2025

Information about the authors:

Deepika Aggarwal – QuNu Labs Pvt. Ltd., M.G. Road, Bangalore, Karnataka, India; ORCID 0000-0003-3238-382X; deepika@qnulabs.com

Anindita Banerjee – QuNu Labs Pvt. Ltd., M.G. Road, Bangalore, Karnataka, India; anindita@qnulabs.com

Ankush Sharma – QuNu Labs Pvt. Ltd., M.G. Road, Bangalore, Karnataka, India; ankush@qnulabs.com

Ganesh Yadav – QuNu Labs Pvt. Ltd., M.G. Road, Bangalore, Karnataka, India; ganesh@qnulabs.com

Conflict of interest: the authors declare no conflict of interest.